Windows Store & Apps (APPX) analysis

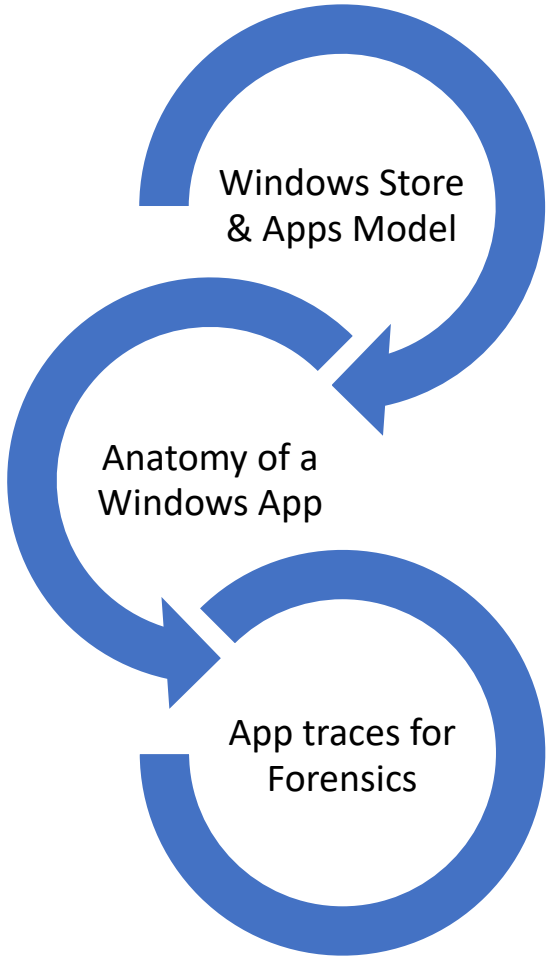
@jackfarley248
@swiftforensics

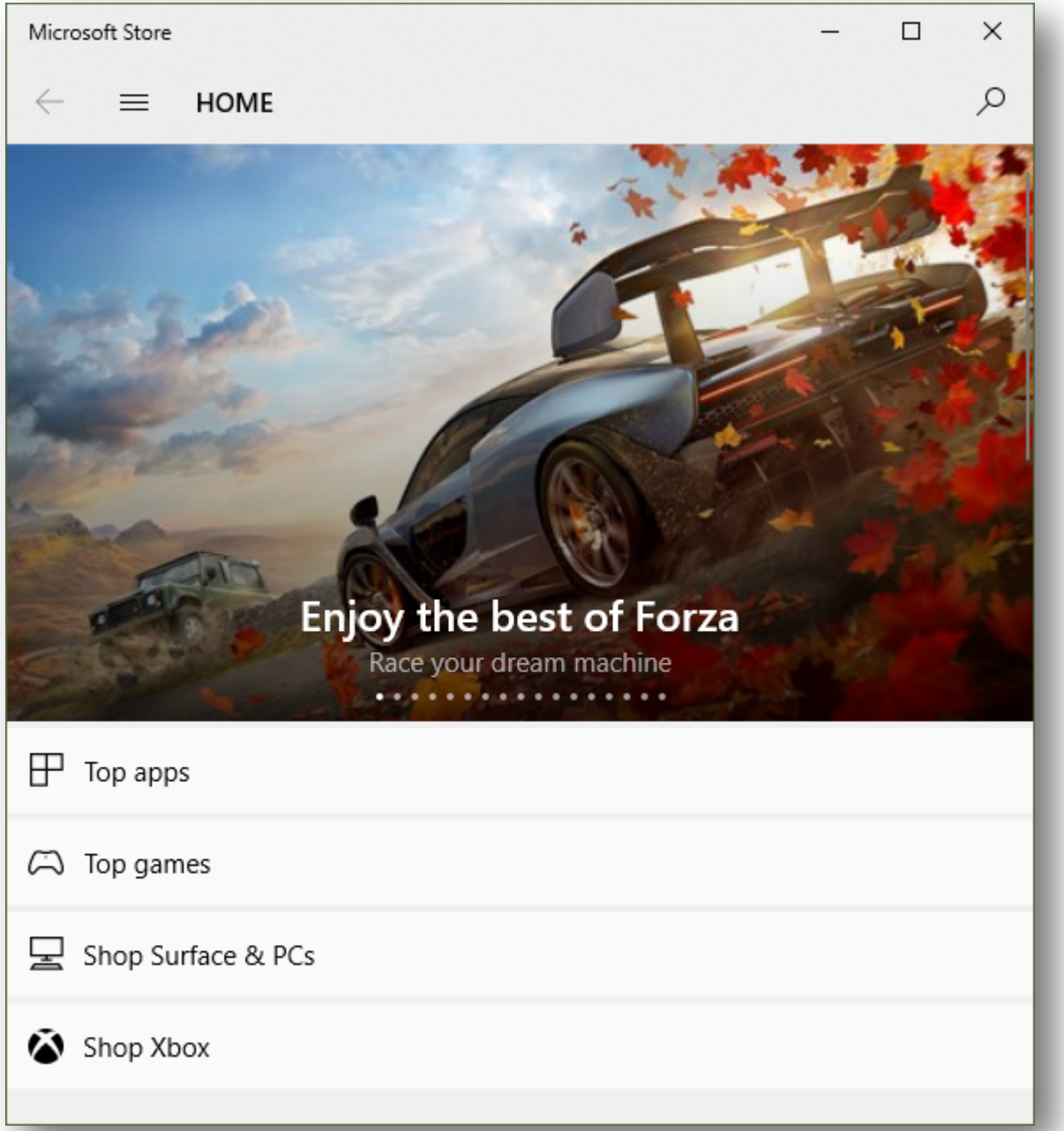
Yogesh Khatri

Jack Farley

Champlain College

Agenda


Windows Store
& Apps Model
Anatomy of a
Windows App
App traces for
Forensics

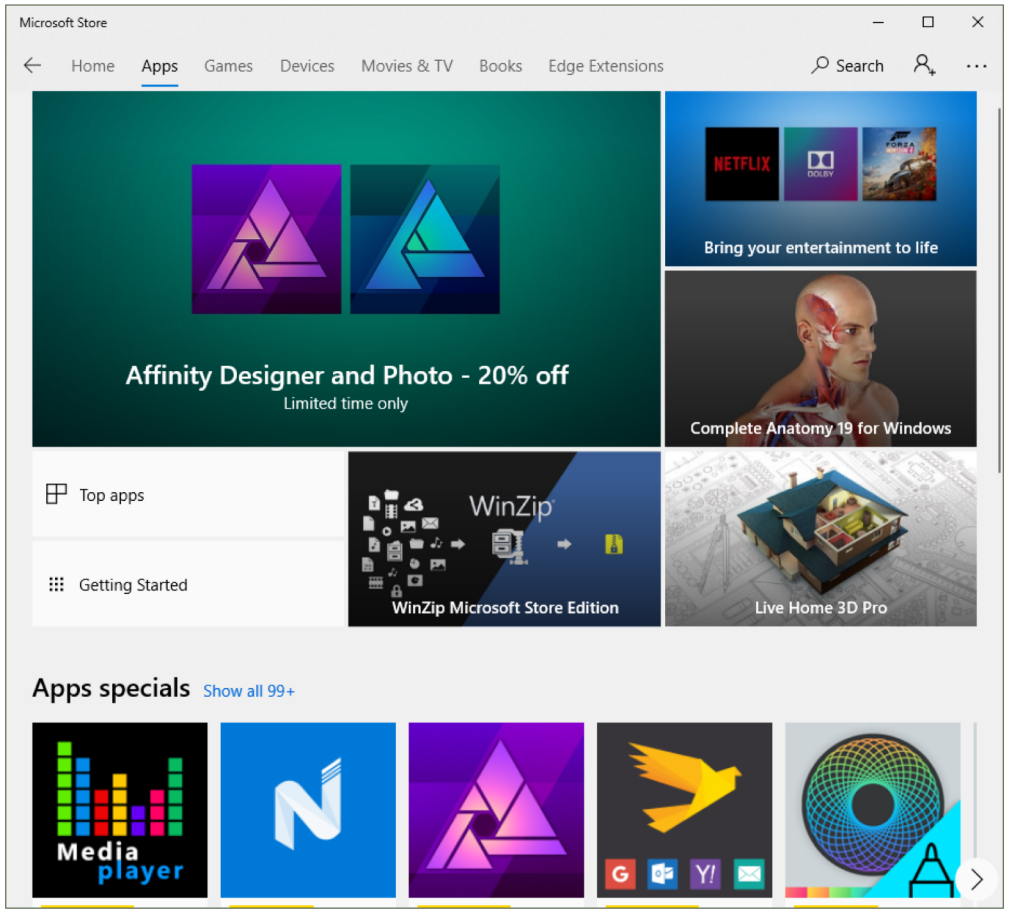

Microsoft Store
HOME
Enjoy the best of Forza
Race your dream machine
Top apps
Top games
Shop Surface & PCs
Shop Xbox

Universal Windows Platform – UWP

UWP apps were earlier called Metro Apps (windows 8), Modern Apps, then Universal Apps (windows 10)

https://docs.microsoft.com/en-us/windows/uwp/get-started/universal-application-platform-guide

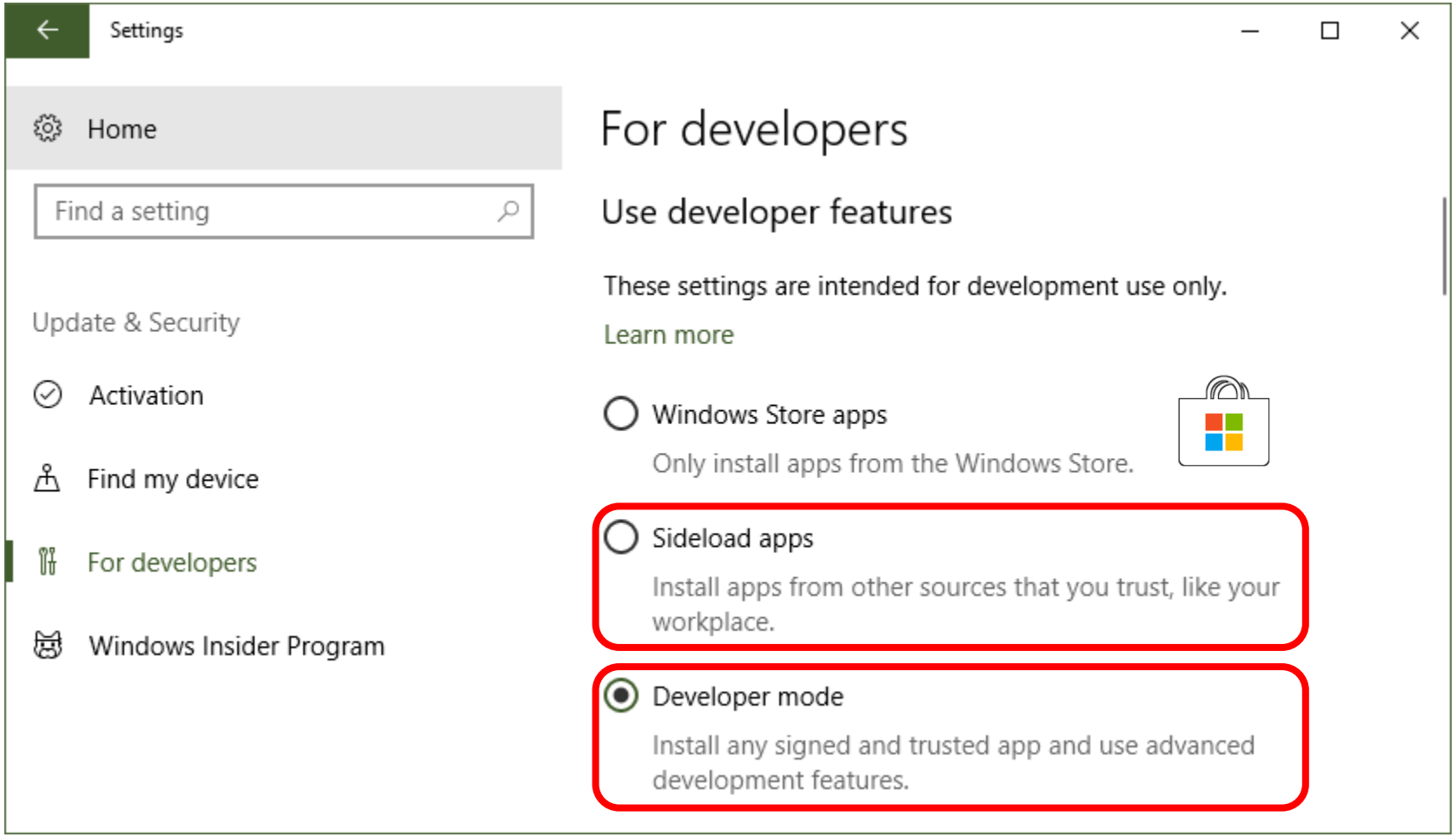
UWP App Model



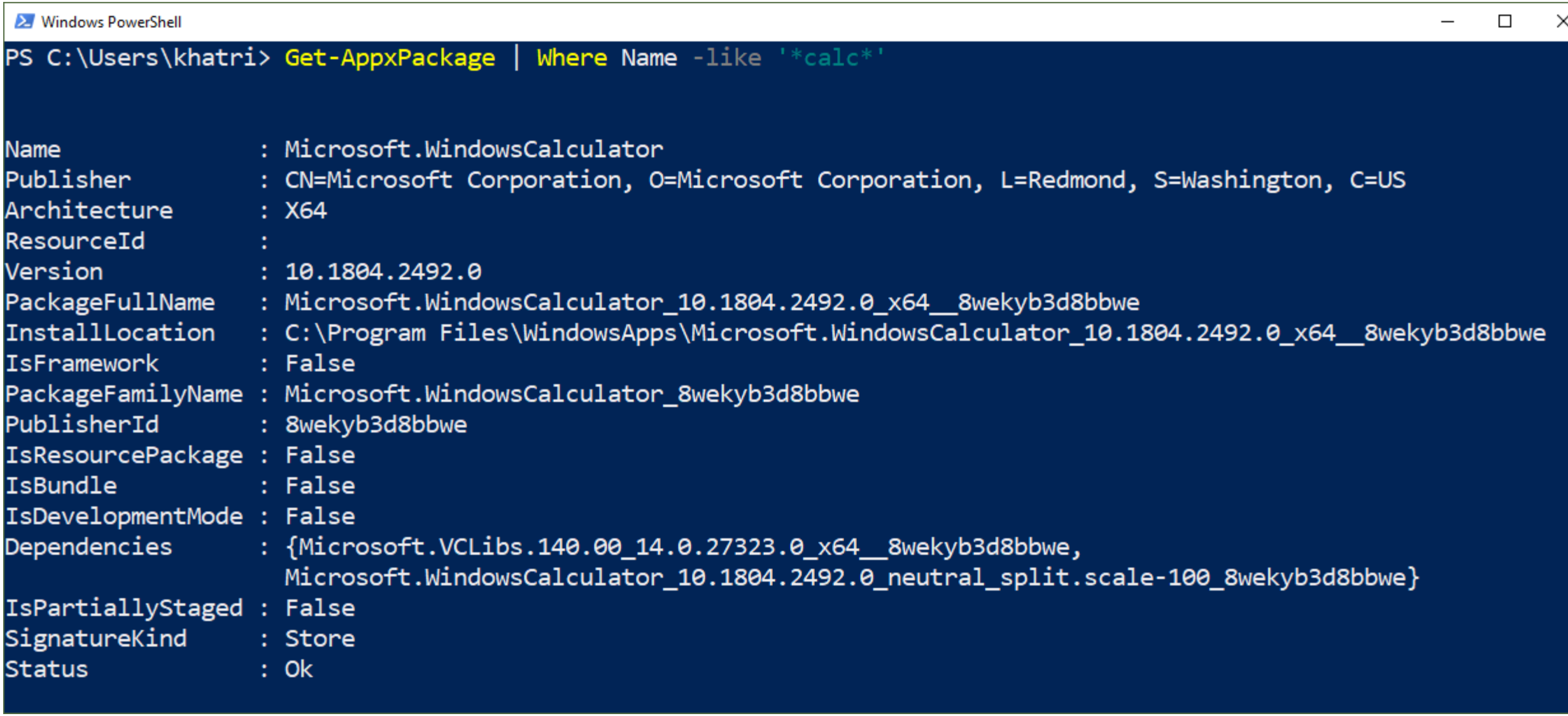
- Downloads as APPX package
- Secure App delivery (via Microsoft Store)
- Runs in Sandboxed environment
  - No registry access
  - No file system access outside sandbox folder
  - Must use Windows Runtime API (winRT)
    - Very limited win32 API access
  - Apps must declare device resources used (microphone, camera, ..)
- Apps can interact with Windows Timeline, Cortana, Live tiles, send Push Notifications

Installing AppX outside the Store

- Sideloading allows trusted apps only!
- Dev mode allows any untrusted app



Getting Appx info on live machines



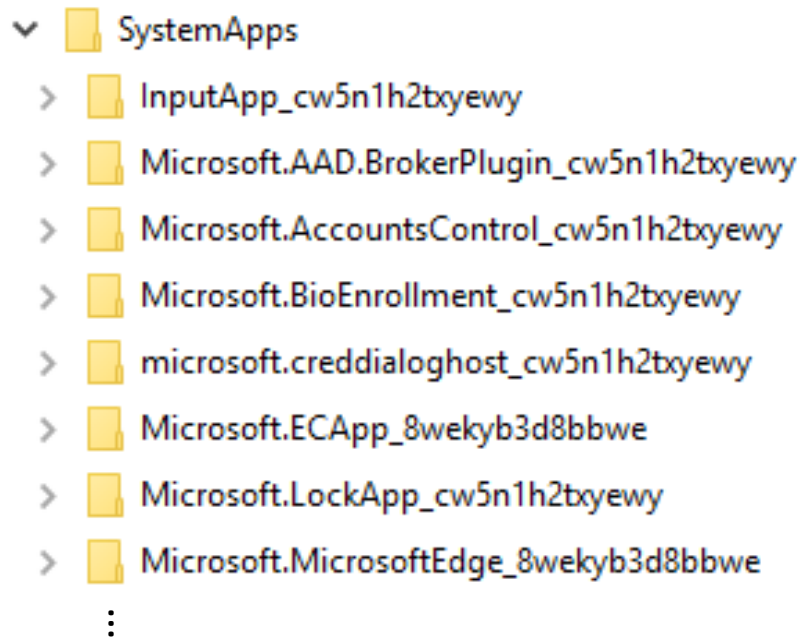
Application Identity

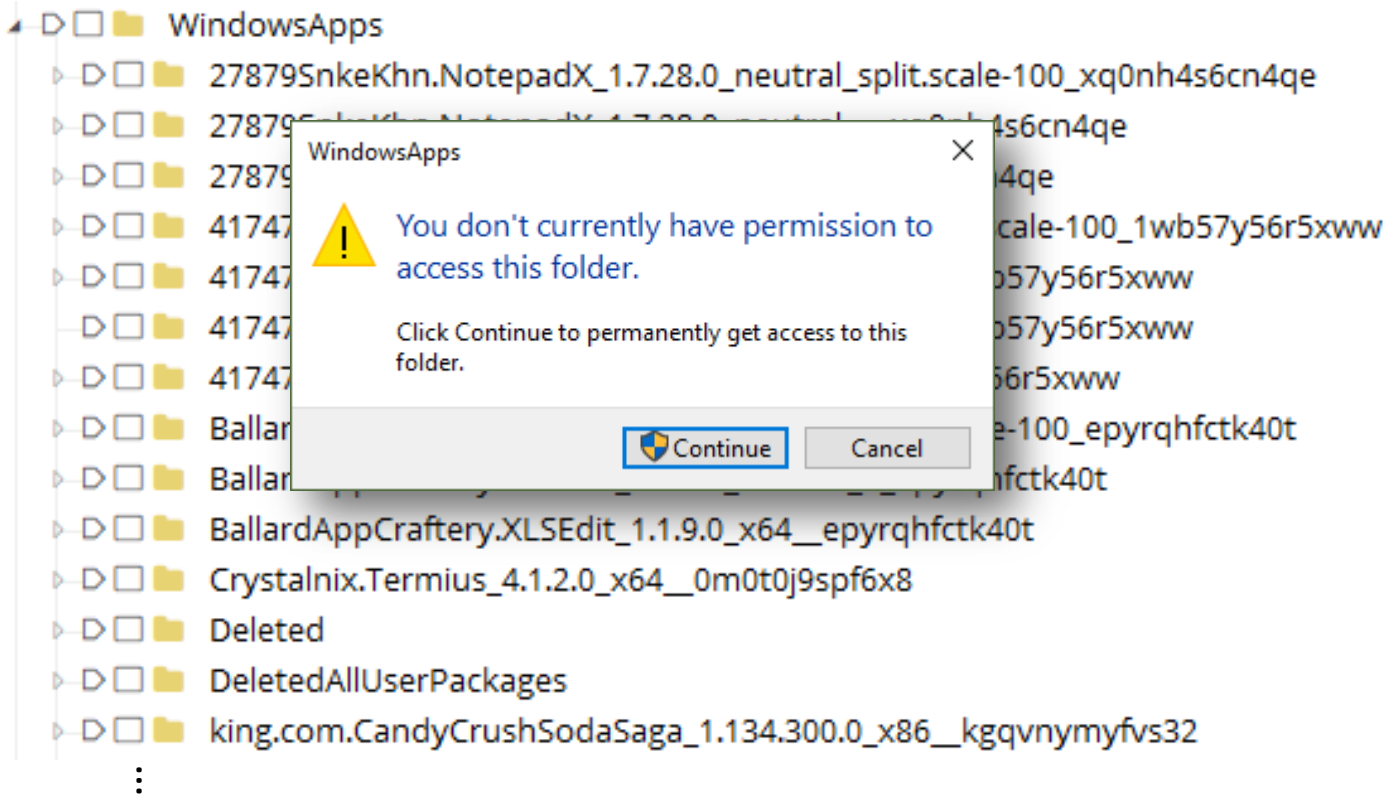
Item	Value
Publisher Name	CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Publisher ID	8wekyb3d8bbwe
Architecture	X64
Version	10.1804.2492.0
Package Name	Microsoft.WindowsCalculator
Package Family Name	Microsoft.WindowsCalculator_8wekyb3d8bbwe
Package Full Name	Microsoft.WindowsCalculator_10.1804.2492.0_x64__8wekyb3d8bbwe
Package-Relative App ID	App
Application User Model ID (AUMID)	Microsoft.WindowsCalculator_8wekyb3d8bbwe!App

App installation Locations

Folder Owned by *TrustedInstaller*
S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464

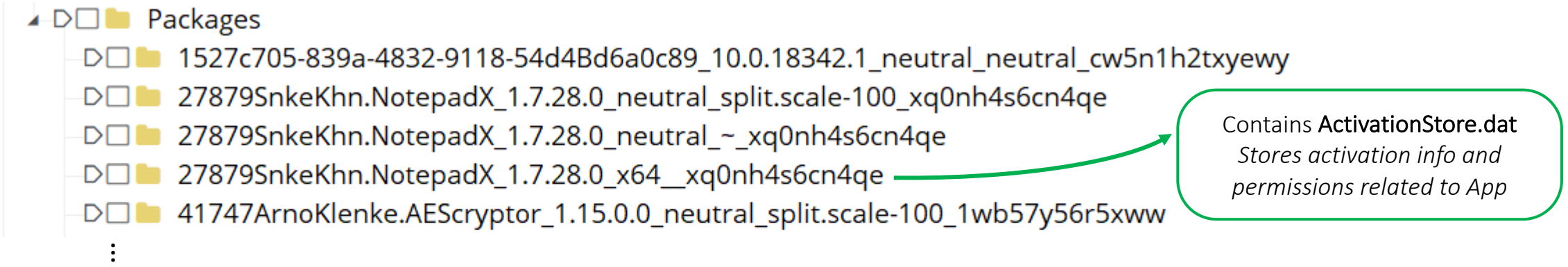
- C:\Windows\SystemApps
- C:\Program Files\WindowsApps





Package Activation Databases & Capability

- C:\ProgramData\Microsoft\Windows\AppRepository\Packages



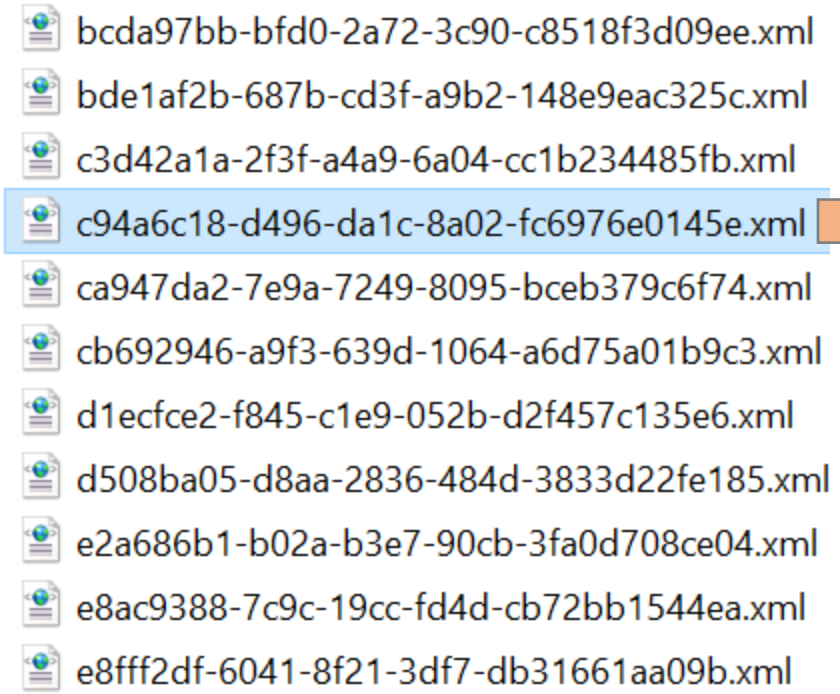
- Capabilities listed in .xml files in Packages folder

```
<Capabilities>
    <Capability Name="internetClient"/>
    <uap:Capability Name="videosLibrary"/>
    <uap:Capability Name="picturesLibrary"/>
    <DeviceCapability Name="microphone"/>
    <DeviceCapability Name="webcam"/>
    <DeviceCapability Name="location"/>
</Capabilities>
```

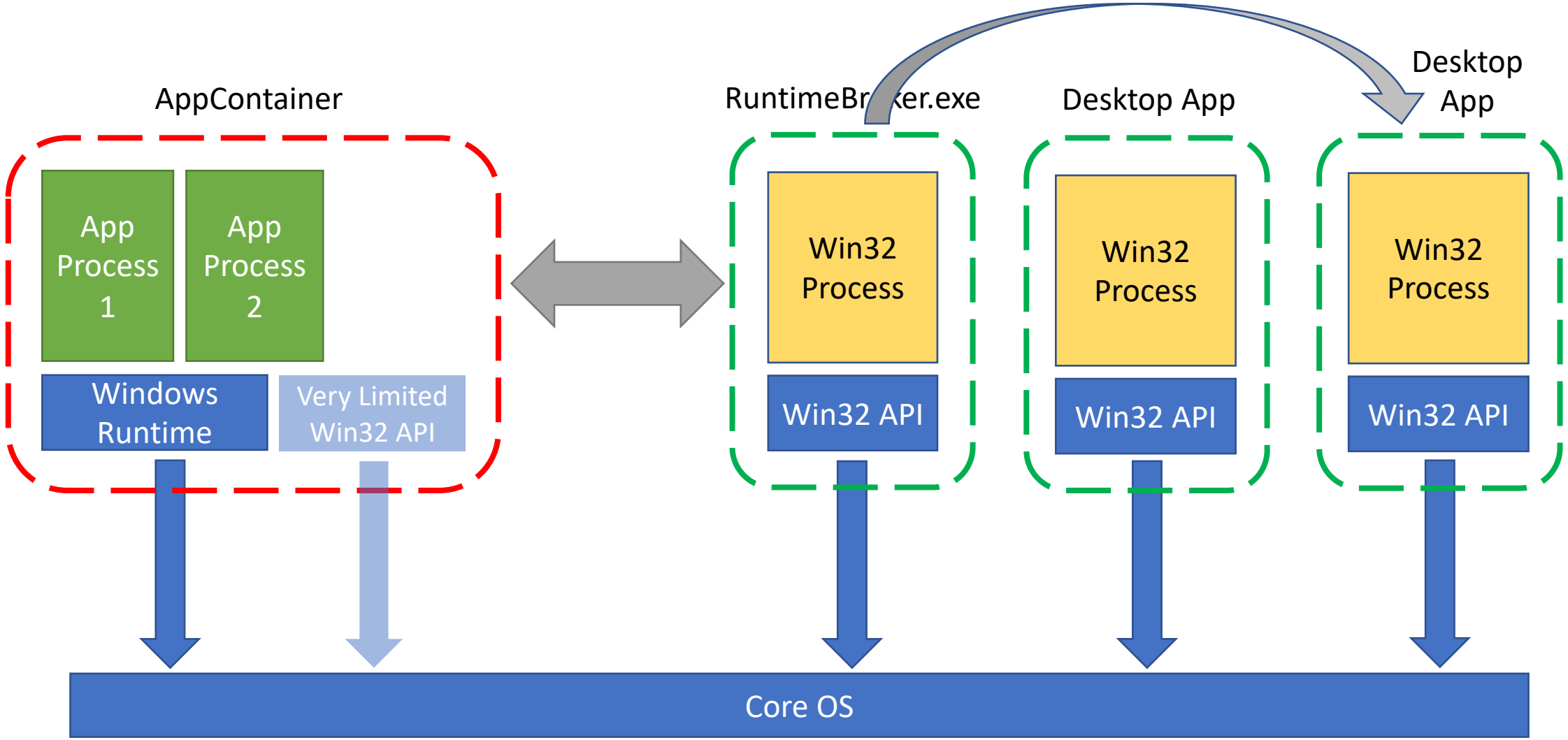
Capabilities of Windows 10 Camera App listed in C:\ProgramData\Microsoft\Windows\AppRepository\Microsoft.WindowsCamera_2019.124.40.0_x64__8wekyb3d8bbwe.xml

Package licensing info

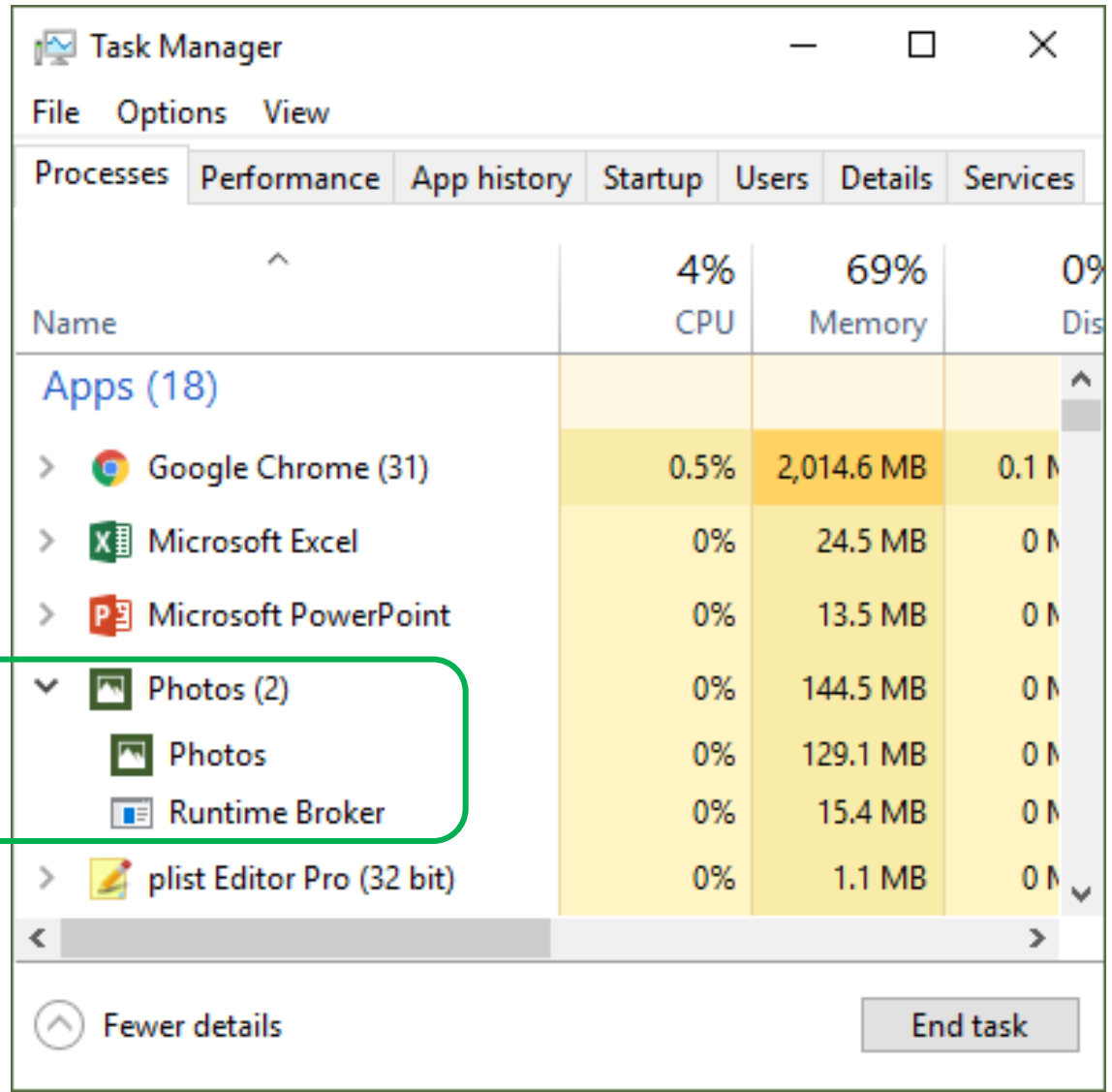
- C:\ProgramData\Microsoft\Windows\ClipSVC\Archive\Apps\

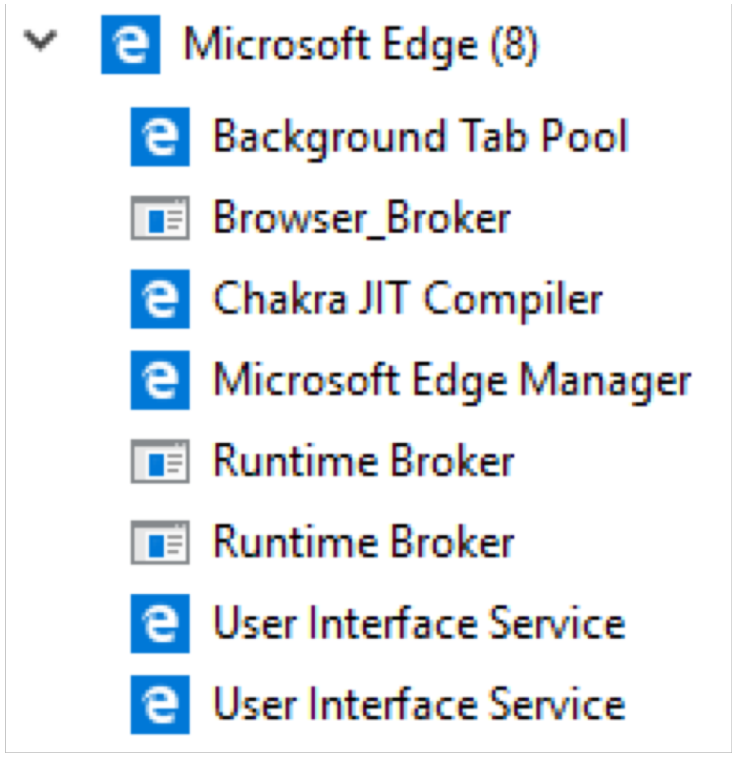


AppContainer



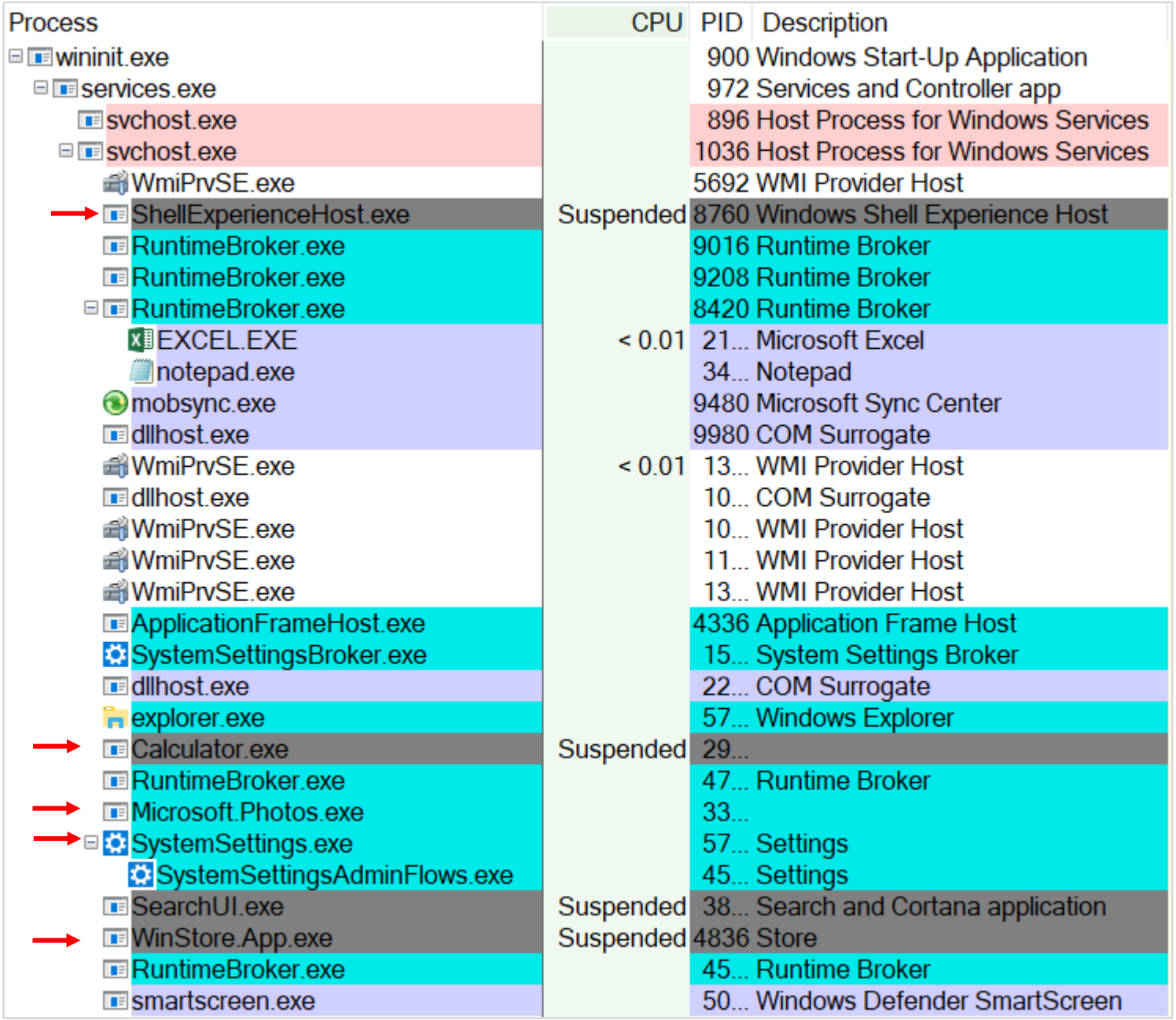
App processes





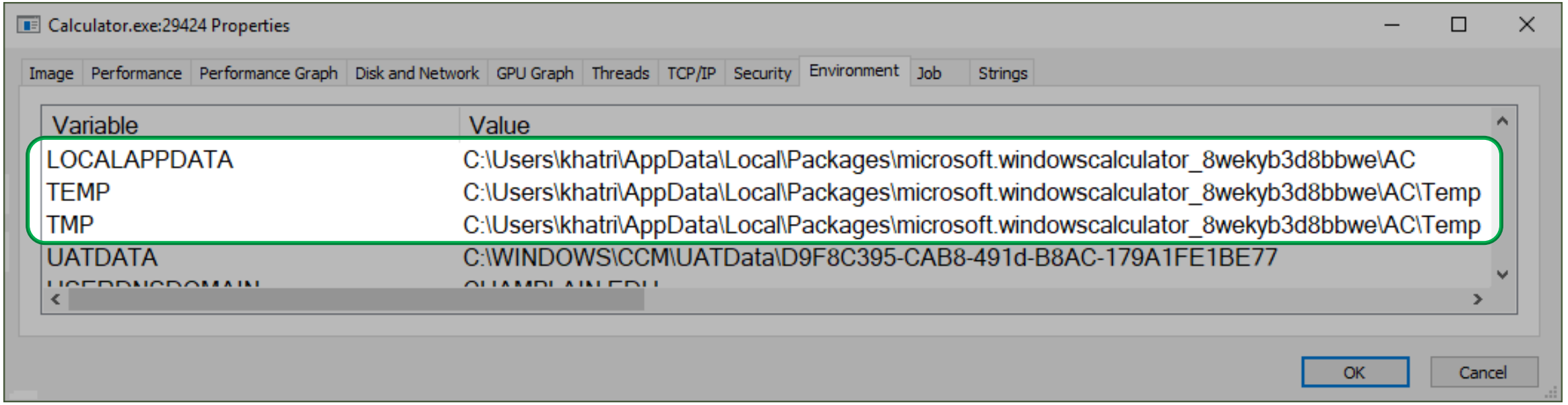
Process Details

- Svchost is Parent process for all APPs
- Applications launched cannot be traced back to parent APP



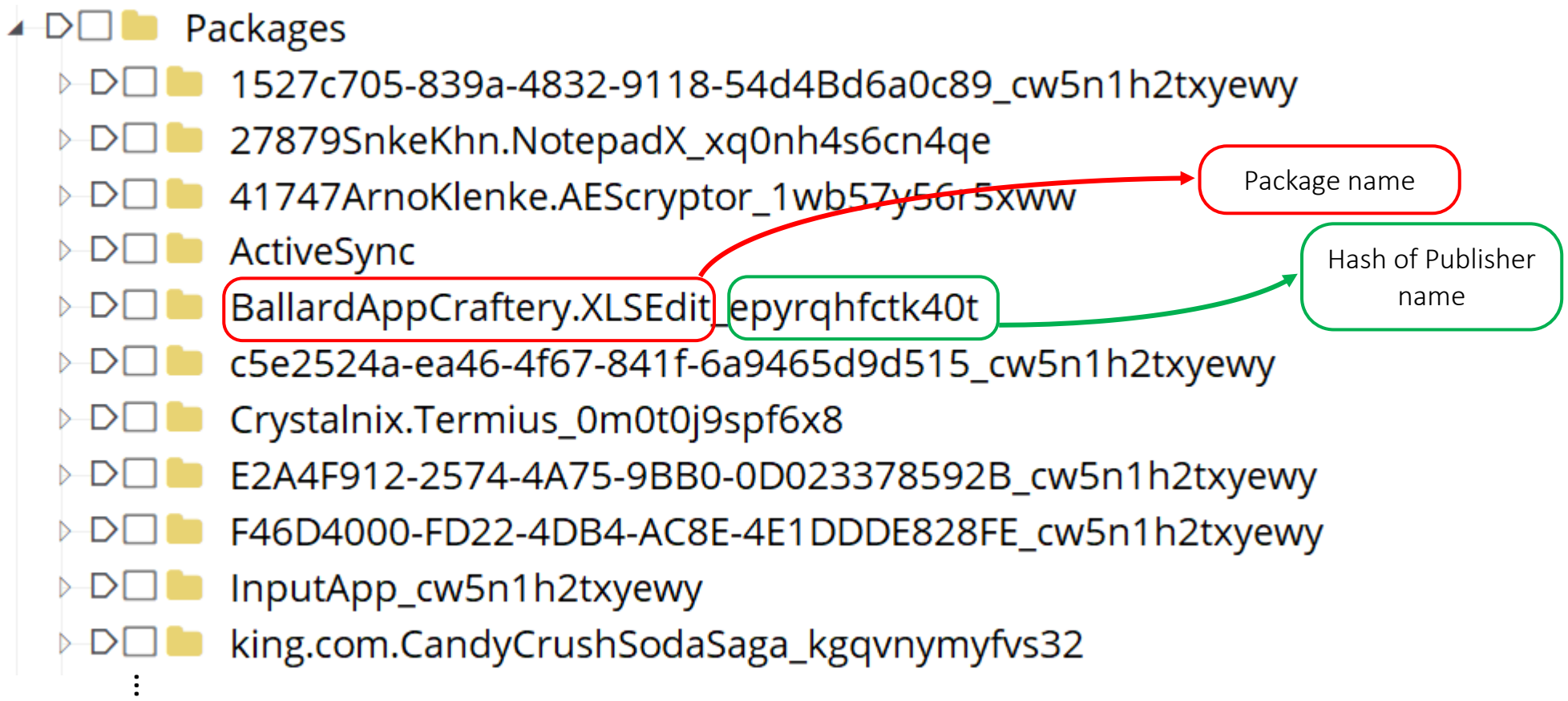
Process	CPU	PID	Description
wininit.exe		900	Windows Start-Up Application
services.exe		972	Services and Controller app
svchost.exe		896	Host Process for Windows Services
svchost.exe		1036	Host Process for Windows Services
WmiPrvSE.exe		5692	WMI Provider Host
ShellExperienceHost.exe	Suspended	8760	Windows Shell Experience Host
RuntimeBroker.exe		9016	Runtime Broker
RuntimeBroker.exe		9208	Runtime Broker
RuntimeBroker.exe		8420	Runtime Broker
EXCEL.EXE	< 0.01	21...	Microsoft Excel
notepad.exe		34...	Notepad
mobsync.exe		9480	Microsoft Sync Center
dllhost.exe		9980	COM Surrogate
WmiPrvSE.exe	< 0.01	13...	WMI Provider Host
dllhost.exe		10...	COM Surrogate
WmiPrvSE.exe		10...	WMI Provider Host
WmiPrvSE.exe		11...	WMI Provider Host
WmiPrvSE.exe		13...	WMI Provider Host
ApplicationFrameHost.exe		4336	Application Frame Host
SystemSettingsBroker.exe		15...	System Settings Broker
dllhost.exe		22...	COM Surrogate
explorer.exe		57...	Windows Explorer
Calculator.exe	Suspended	29...	
RuntimeBroker.exe		47...	Runtime Broker
Microsoft.Photos.exe		33...	
SystemSettings.exe		57...	Settings
SystemSettingsAdminFlows.exe		45...	Settings
SearchUI.exe	Suspended	38...	Search and Cortana application
WinStore.App.exe	Suspended	4836	Store
RuntimeBroker.exe		45...	Runtime Broker
smartscreen.exe		50...	Windows Defender SmartScreen

Process Environment Variables



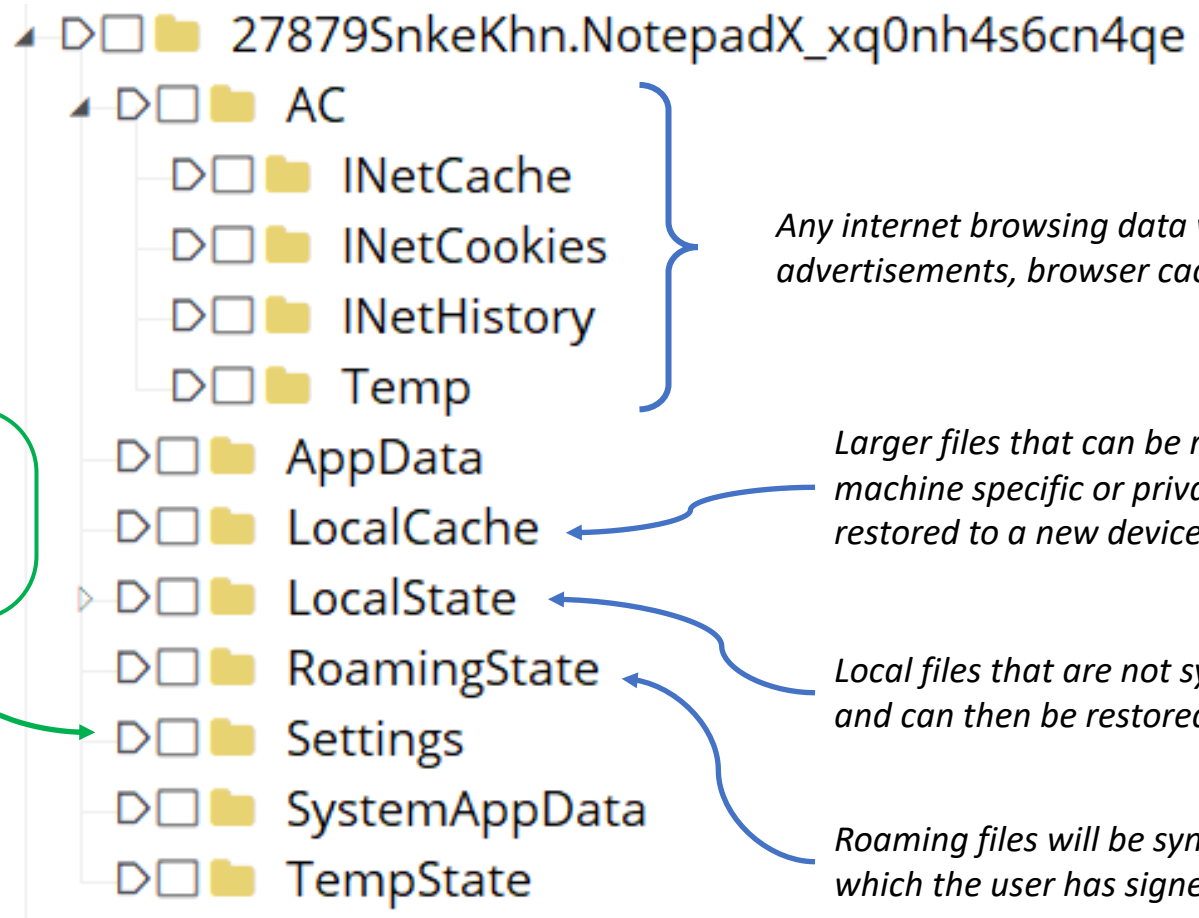
Per user artifacts

- C:\Users*<USER>*\AppData\Local\Packages



App Data – Notepad X as example

Notepad X App's folder in %LocalAppData%\Packages



Any internet browsing data will land up here (In-app advertisements, browser caches, cookies)

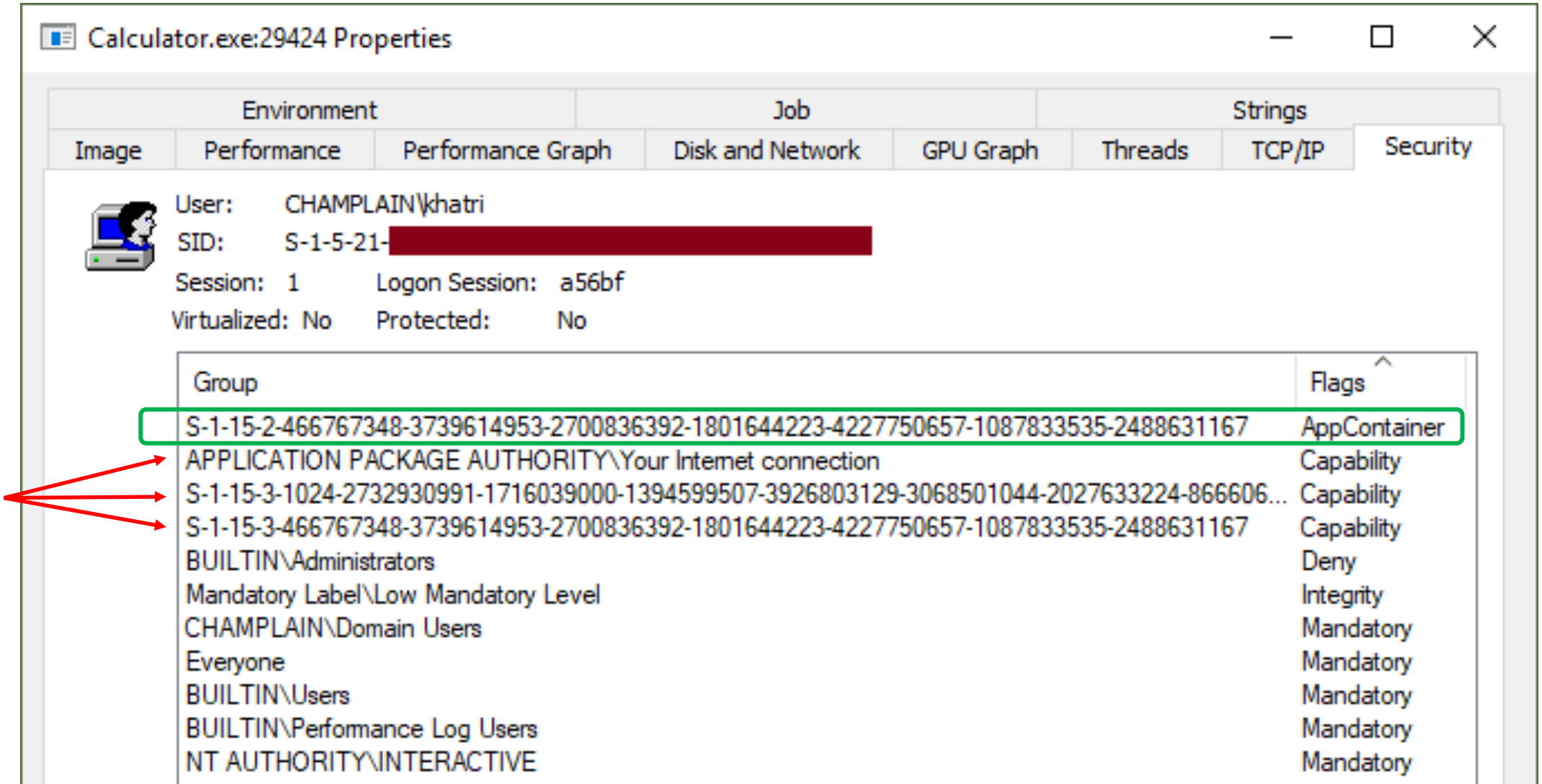
Contains **Settings.dat**
Stores Local & Roaming settings for the App

Larger files that can be recreated by the app, and for machine specific or private files that should not be restored to a new device

Local files that are not synchronized, but are backed up, and can then be restored to another device

Roaming files will be synchronized across machines on which the user has signed in with a connected account

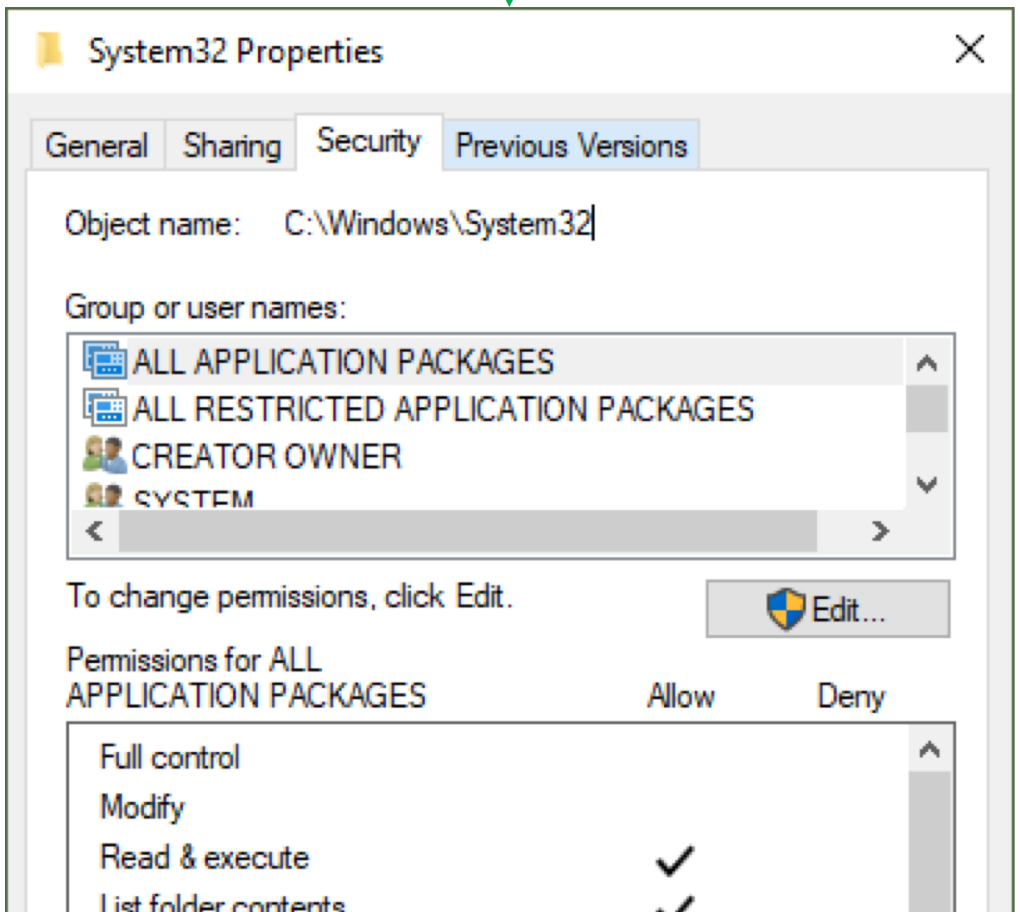
AppContainer & Capability SIDs



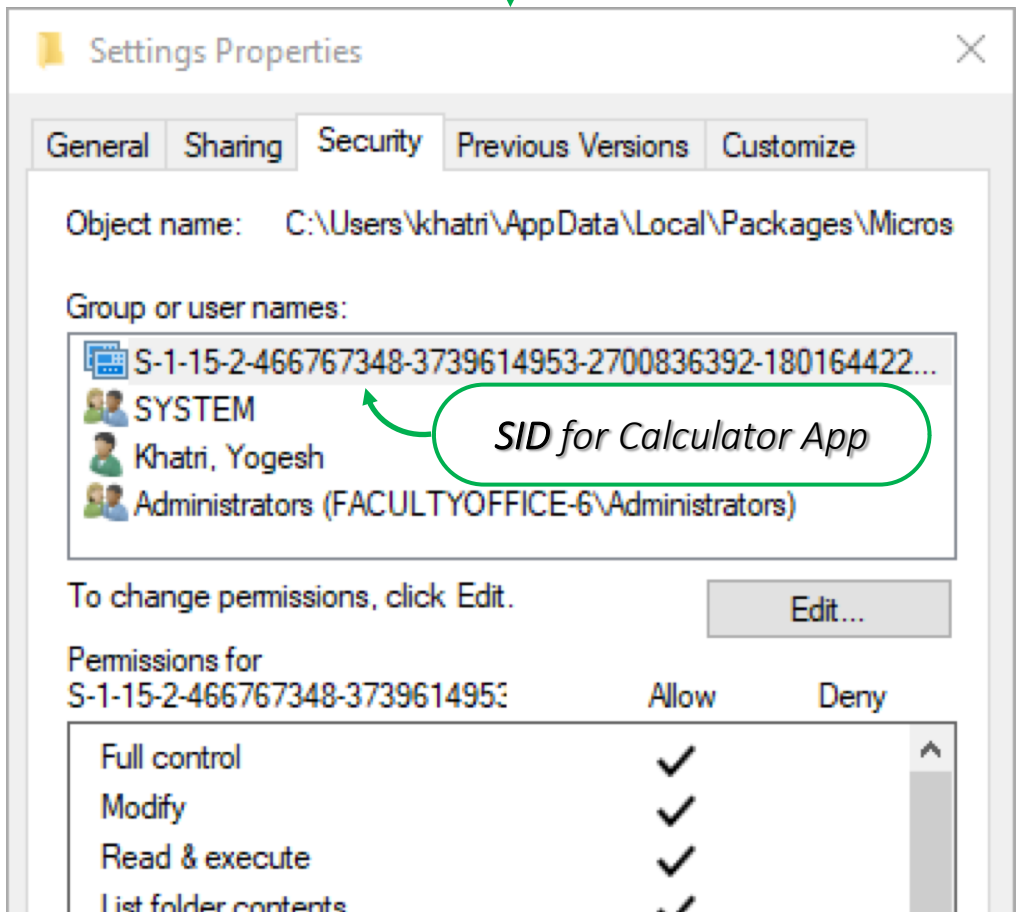
Capabilities

SID Permissions

C:\Windows\System32



%LocalAppData%\Packages\Microsoft.WindowsCalculator_8wekyb3d8bbwe\Settings

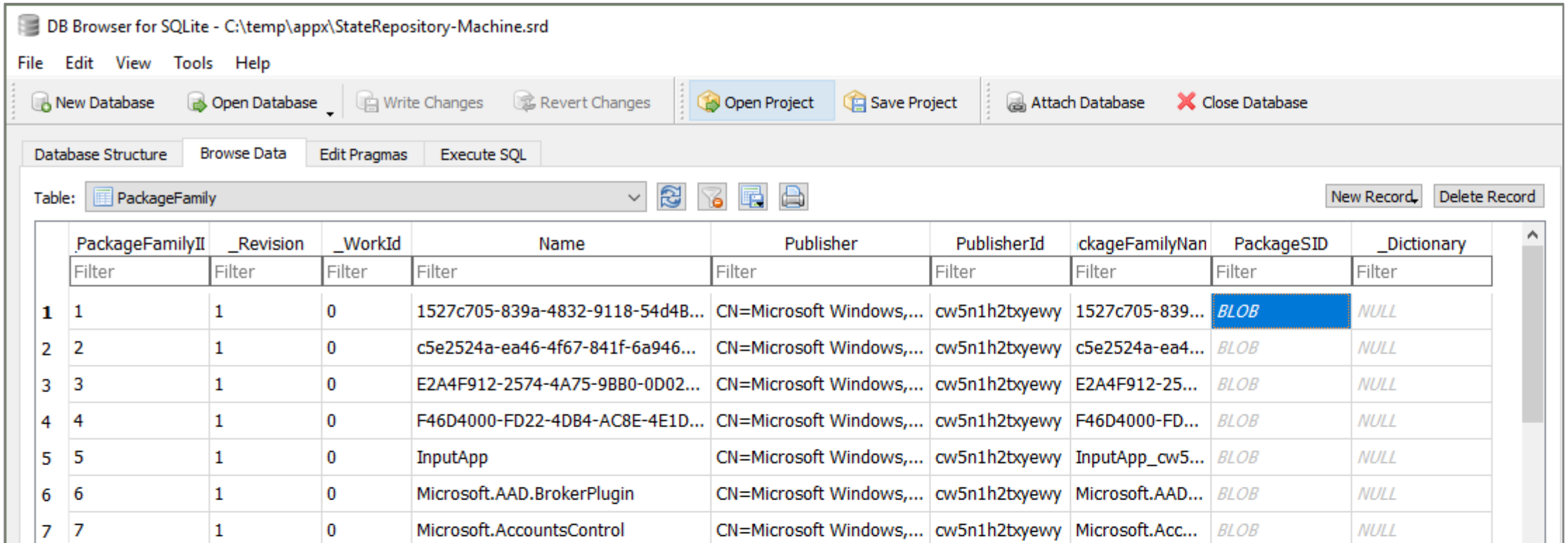


Lets do some Forensics!

- Get information about installed apps
  - Install/Uninstall dates
  - Locations
  - Usage information
    - App settings
    - Execution traces
    - Files/Folders accessed
- Look for uninstalled app remains

Installed App info

- C:\ProgramData\Microsoft\Windows\AppRepository\Packages
  - StateRepository-Machine.srd
  - StateRepository-Deployment.srd



	PackageFamilyII	_Revision	_WorkId	Name	Publisher	PublisherId	ckageFamilyNan	PackageSID	_Dictionary
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1	0	1527c705-839a-4832-9118-54d4B...	CN=Microsoft Windows,...	cw5n1h2txyewy	1527c705-839...	BLOB	NULL
2	2	1	0	c5e2524a-ea46-4f67-841f-6a946...	CN=Microsoft Windows,...	cw5n1h2txyewy	c5e2524a-ea4...	BLOB	NULL
3	3	1	0	E2A4F912-2574-4A75-9BB0-0D02...	CN=Microsoft Windows,...	cw5n1h2txyewy	E2A4F912-25...	BLOB	NULL
4	4	1	0	F46D4000-FD22-4DB4-AC8E-4E1D...	CN=Microsoft Windows,...	cw5n1h2txyewy	F46D4000-FD...	BLOB	NULL
5	5	1	0	InputApp	CN=Microsoft Windows,...	cw5n1h2txyewy	InputApp_cw5...	BLOB	NULL
6	6	1	0	Microsoft.AAD.BrokerPlugin	CN=Microsoft Windows,...	cw5n1h2txyewy	Microsoft.AAD...	BLOB	NULL
7	7	1	0	Microsoft.AccountsControl	CN=Microsoft Windows,...	cw5n1h2txyewy	Microsoft.Acc...	BLOB	NULL

Query to extract App information

```
SELECT DISTINCT * FROM
(SELECT substr(packfam.PackageFamilyName, instr(packfam.PackageFamilyName, '.') + 1,
         instr(packfam.PackageFamilyName, '_') -2 - instr(packfam.PackageFamilyName, '.') + 1 ) as AppName,
  datetime((packuser.installTime/10000000) -11644473600, 'unixepoch') InstallTime,
  CASE WHEN instr(pack.PublisherDisplayName, 'ms-resource')=0 THEN pack.PublisherDisplayName
      ELSE '' END AS PublisherDisplayName,
  packfam.PublisherId, packuser.User, userkey.UserSid,
  CASE Architecture
    WHEN 0 THEN 'X64'
    WHEN 9 THEN 'x86'
    WHEN 11 THEN 'Neutral'
    ELSE Architecture END AS Architecture,
  substr(pack.packageFullName, instr(pack.packageFullName, '_') + 1,
         instr(substr(pack.packageFullName, instr(pack.packageFullName, '_') + 1), '_') - 1) AS version,
  CASE SignatureOrigin
    WHEN 3 THEN 'System'
    WHEN 2 THEN 'Store'
    ELSE 'Unknown' END AS SignatureKind,
  packloc.installedLocation
  FROM PackageUser packuser, package pack, MrtPackage mrt, packageFamily packfam, packageLocation packloc, User userkey
  WHERE packuser.package = pack._PackageId
    AND pack.packageFamily = packfam._PackagefamilyId
    AND packuser.user = userkey._UserID
    AND packloc.package = pack._packageId
    AND (pack.resourceId IS NULL OR pack.resourceId = 'neutral')
)
```

This is a modified version of the original query written by Mark McKinnon
This works in all versions of Windows 10 including 19H1

Query Output

AppName	InstallTime	PublisherDisplayName	PublisherId	User	UserSid	Architecture	Version	SignatureKind	inst
WindowsFeedbackHub	2018-09-07 11:27:06	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	1.1805.2331.0	Store	C:\Program File
MicrosoftOfficeHub	2018-09-08 10:43:44	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	17.10314.317...	Store	C:\Program File
WindowsAlarms	2018-09-08 10:44:17	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.1804.1101...	Store	C:\Program File
People	2018-09-08 10:45:55	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.3.3472.2000	Store	C:\Program File
WindowsSoundRecorder	2018-09-08 10:46:43	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.1804.911....	Store	C:\Program File
WindowsCalculator	2018-09-18 23:23:01	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	10.1804.2492.0	Store	C:\Program File
Print3D	2018-09-27 09:11:37	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	3.1.2612.0	Store	C:\Program File
Getstarted	2018-10-09 09:23:19	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	6.15.12641.0	Store	C:\Program File
WindowsMaps	2018-10-13 19:08:50	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	5.1809.2762.0	Store	C:\Program File
Messaging	2018-11-08 20:42:41	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	4.1810.2922.0	Store	C:\Program File
OneConnect	2018-11-17 01:30:51	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	3.1811.3082.0	Store	C:\Program File
XboxIdentityProvider	2018-12-04 15:12:42	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	12.46.25001.0	Store	C:\Program File
Microsoft3DViewer	2018-12-05 12:03:01	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	5.1811.27012.0	Store	C:\Program File
MSPaint	2018-12-05 12:03:27	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	5.1811.20017.0	Store	C:\Program File
MicrosoftSolitaireCollection	2018-12-11 02:18:51	Microsoft Studios	8wekyb3d8bbwe	4	BLOB	X64	4.2.11280.0	Store	C:\Program File
Xbox.TCUI	2018-12-11 02:18:55	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	1.24.10001.0	Store	C:\Program File
BingWeather	2018-12-14 19:25:15	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	4.28.3242.0	Store	C:\Program File
windowscommunicationsapps	2018-12-18 10:43:17	Microsoft Corporation	8wekyb3d8bbwe	4	BLOB	x86	16005.11029....	Store	C:\Program File

All installation History

```
2  select User, HResult,
3  (select PackageFullName from PackageIdentity where PackageIdentity._PackageIdentityID=DeploymentHistory.PackageIdentity) as PkgFullName,
4  datetime((WhenOccurred / 10000000) - 11644473600, 'unixepoch')  when_occurred
5  from DeploymentHistory
```

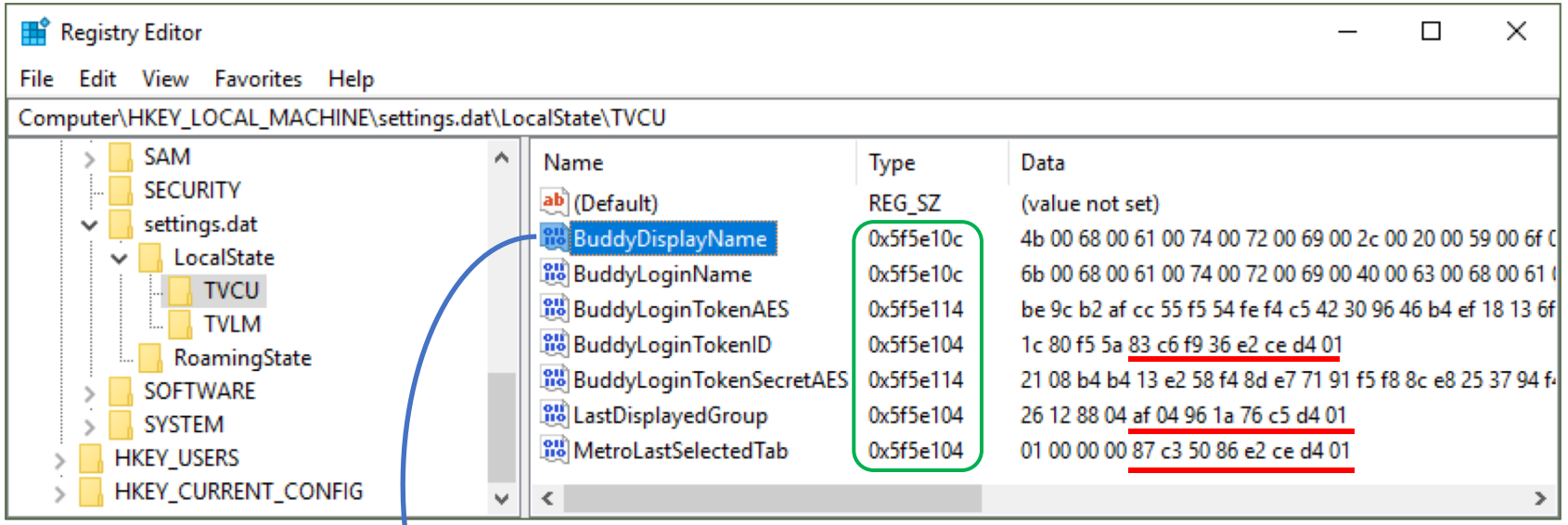
	User	HResult	PkgFullName	when_occurred
167	2	0	Microsoft.BingWeather_4.28.10351.0_neutral_~_8wekyb3d8bbwe	2019-02-15 16:57:19
168	2	0	Microsoft.OneConnect_3.1811.3082.0_neutral_~_8wekyb3d8bbwe	2019-02-15 16:57:49
169	2	0	Microsoft.MicrosoftSolitaireCollection_4.2.11280.0_neutral_~_8wekyb3d8bbwe	2019-02-15 16:59:04
170	2	0	9E2F88E3.Twitter_6.1.4.1000_neutral__wgeqdkkx372wm	2019-02-15 16:59:14
171	2	0	Microsoft.SkypeApp_14.39.180.0_neutral_~_kzf8qxf38zg5c	2019-02-15 17:01:57
172	2	0	king.com.CandyCrushSodaSaga_1.132.300.0_x86__kgqvnymyfvs32	2019-02-15 17:02:00
173	2	0	Microsoft.Windows.Photos_2019.18114.17710.0_neutral_~_8wekyb3d8bbwe	2019-02-15 17:02:07
174	2	0	Microsoft.Windows.CloudExperienceHost_10.0.17134.1_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:48:58
175	2	0	Microsoft.AAD.BrokerPlugin_1000.17134.1.0_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:48:58
176	2	0	Microsoft.Windows.ShellExperienceHost_10.0.17134.112_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:07
177	2	0	windows.immersivecontrolpanel_10.0.2.1000_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:08
178	2	0	Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:09
179	2	0	Microsoft.Windows.ContentDeliveryManager_10.0.17134.1_neutral_neutral_cw5n1h2txyewy	2019-02-15 18:49:10
180	2	0	Microsoft.MicrosoftEdge_42.17134.1.0_neutral__8wekyb3d8bbwe	2019-02-15 18:49:10
181	2	0	microsoft.windowscommunicationsapps_16005.11029.20108.0_neutral_~_8wekyb3d8bbwe	2019-02-15 18:50:32

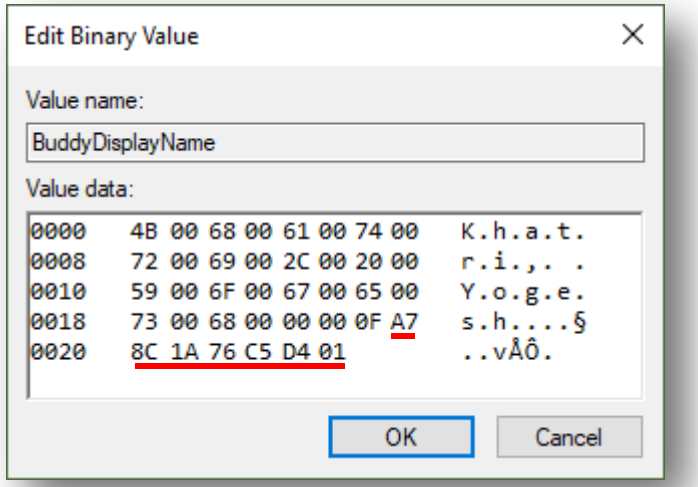
Uninstalled App

App settings from Settings.dat

*Viewing settings.dat using regedit's **Load Hive** option*

The hive is located at %LocalAppData%\Packages\<APP>\Settings





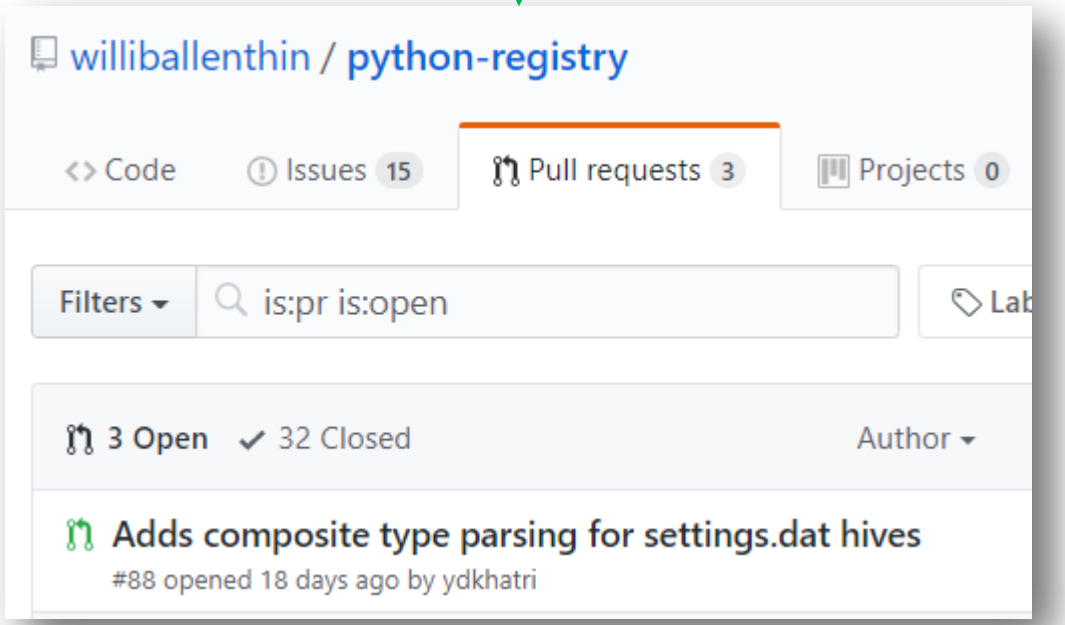
Every Value has a Last Modified timestamp

Settings.dat – New data types

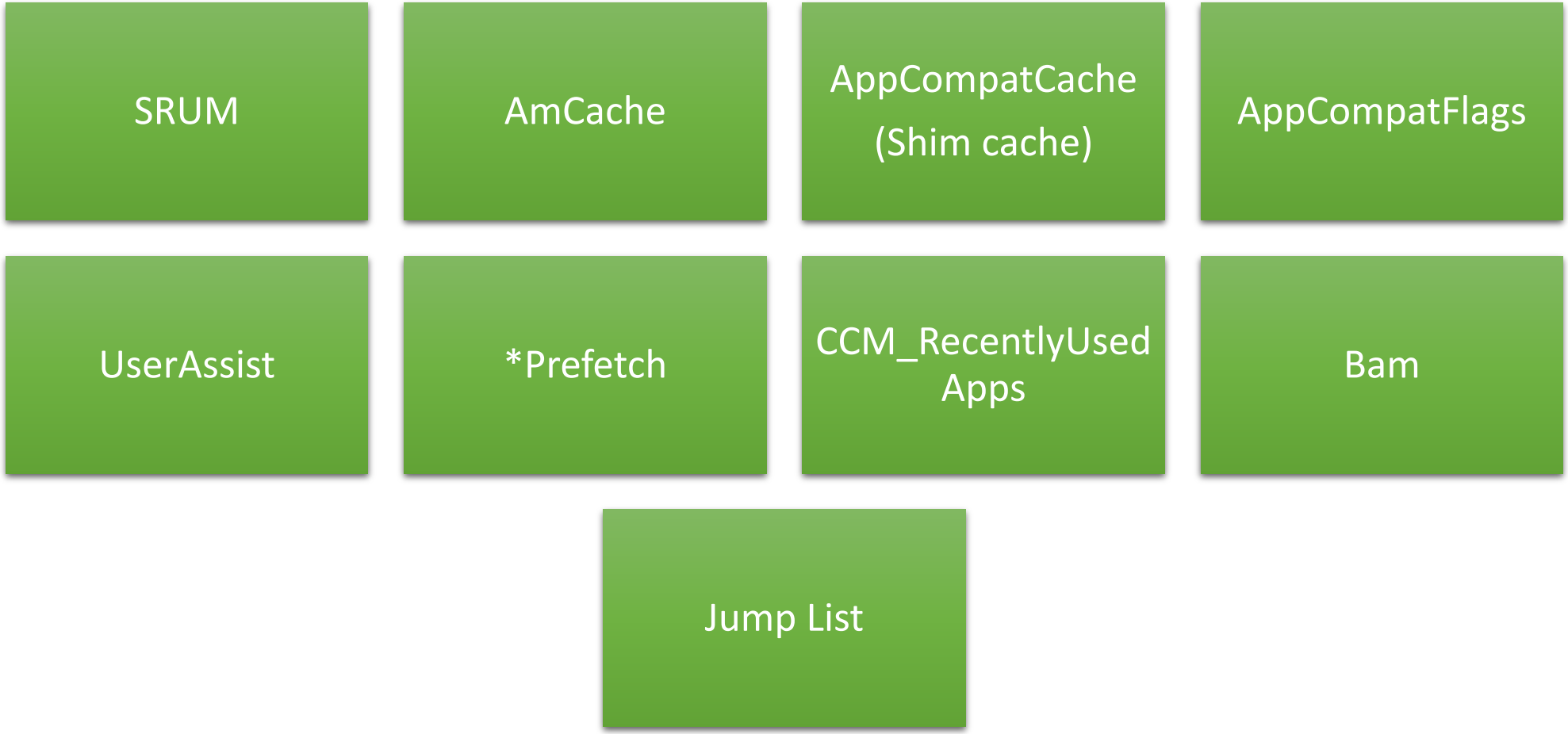
Reg Type Last byte (hex)	Data type
01	uint8
02	int16
03	uint16
04	int32
05	uint32
06	int64
07	uint64
08	Float / Single
09	Double
0A	Unicode char
0B	Boolean
0C	Unicode String
0D	Application Data Composite Value (Dictionary Object)
0E	DateTimeOffset (timestamp)
0F	TimeSpan (100ns ticks)

Reg Type Last byte (hex)	Data Type
10	GUID
11	?
12	?
13	?
14	bytes array
15	int16 array
16	uint16 array
17	int32 array
18	uInt32 array
19	int64 array
1A	uint64 array
1B	Float array
1C	Double array
1D	Unicode char array
1E	Boolean array
1F	Unicode string array

All discovered types added to ***python-registry***

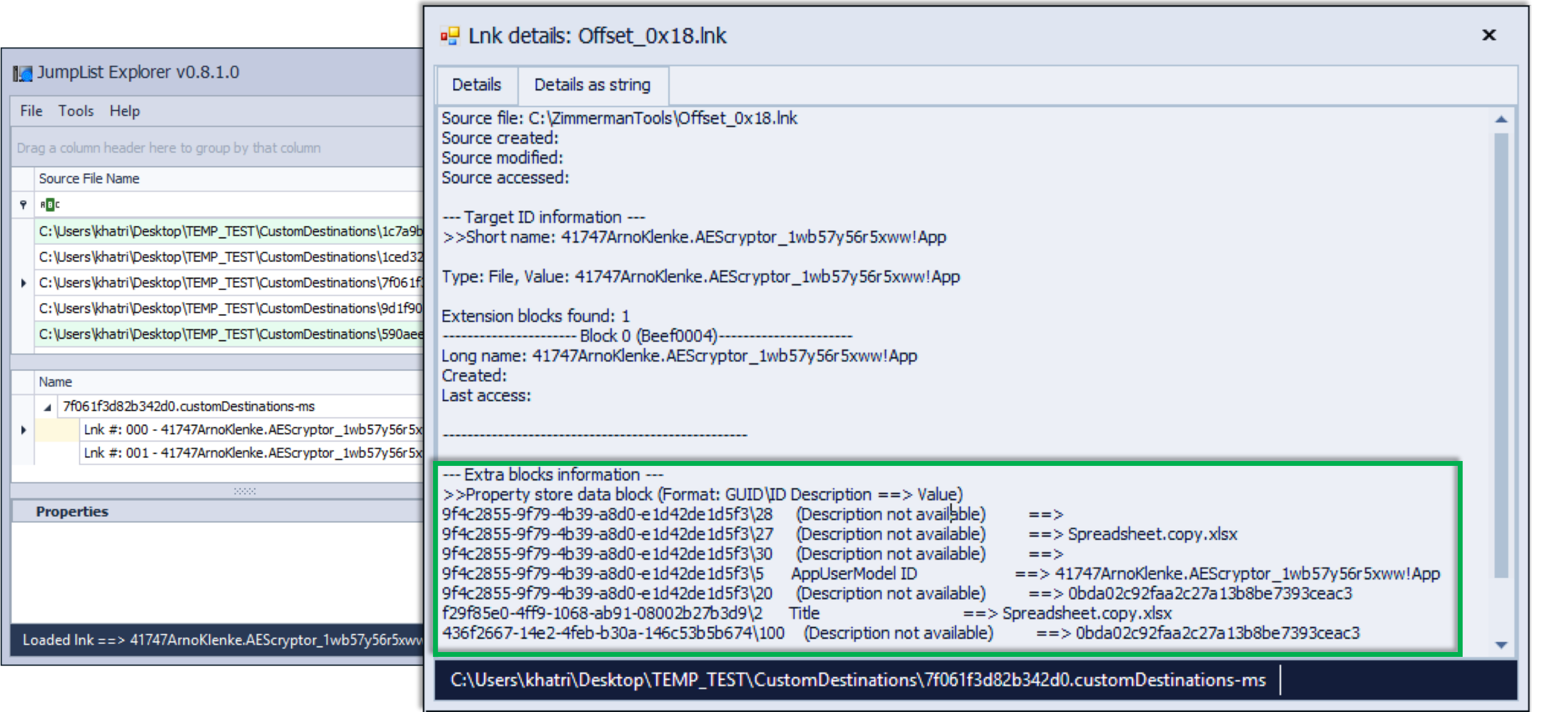


App execution trace artifacts



** Some apps like Twitter do not have an exe*

App execution traces – Jumplist CustomDest



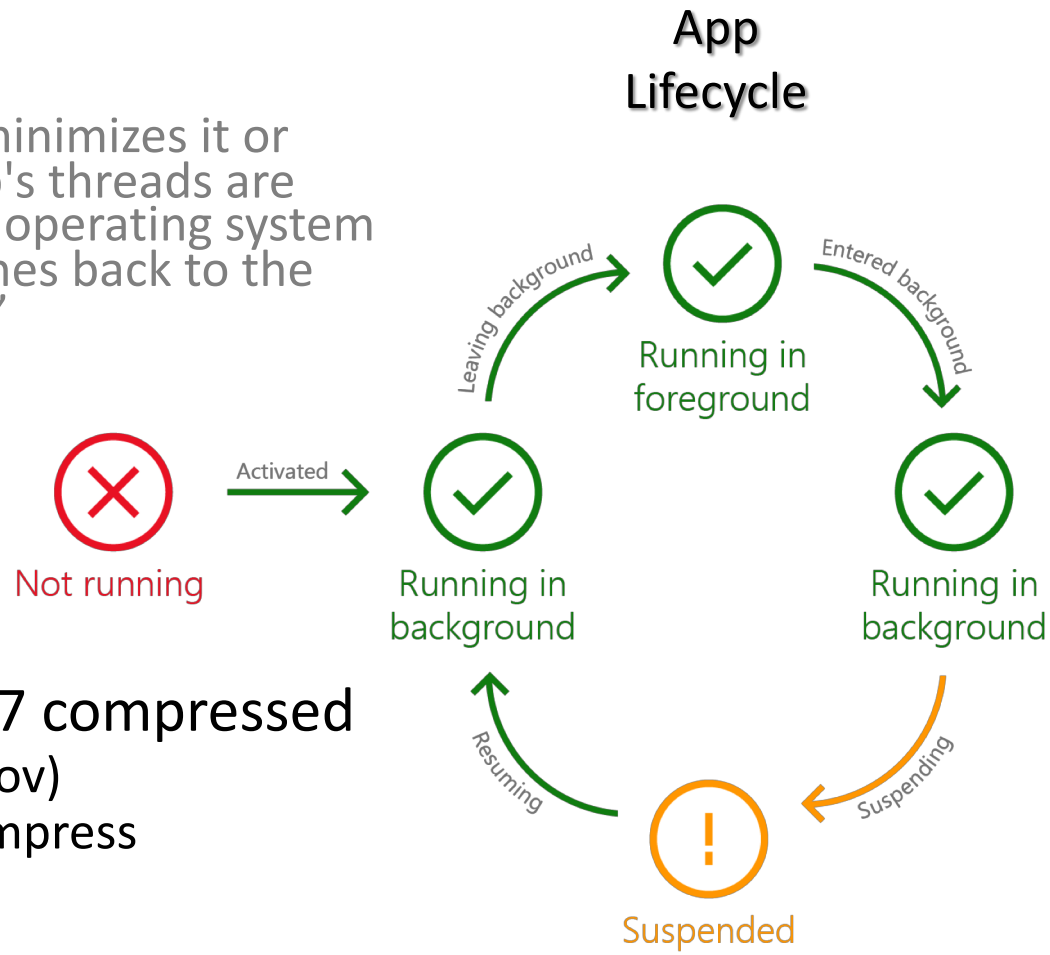
swapfile.sys

- Per Microsoft:

  “A UWP app is suspended shortly after the user minimizes it or switches to another app. This means that the app's threads are stopped and the app is left in memory unless the operating system needs to reclaim resources. When the user switches back to the app, it can be quickly restored to a running state.”

- Suspended app memory pages are moved to **C:\swapfile.sys**

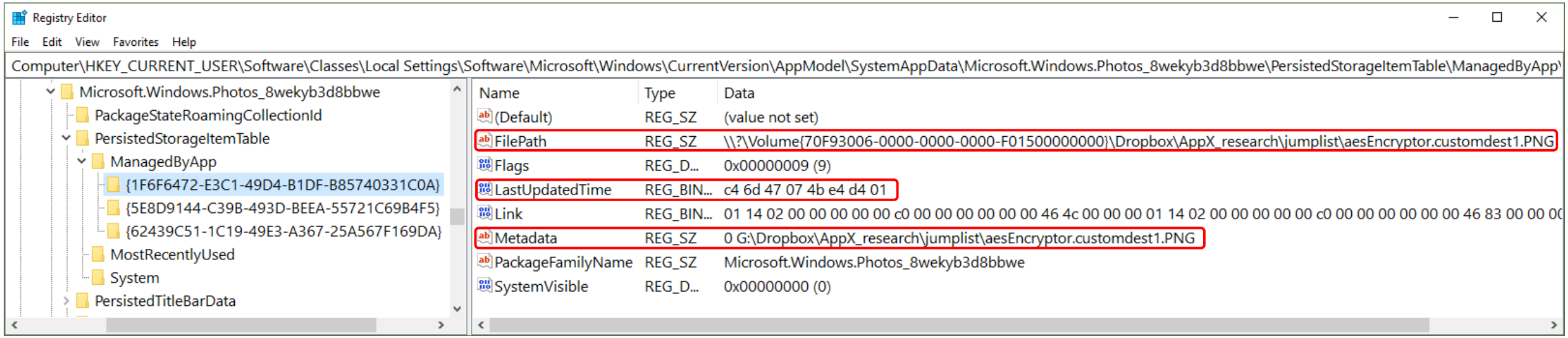
- In windows 10, pages swapped may be LZ77 compressed
  - Use winmem_decompress (from Maxim Suhanov)
  - https://github.com/msuhanov/winmem_decompress



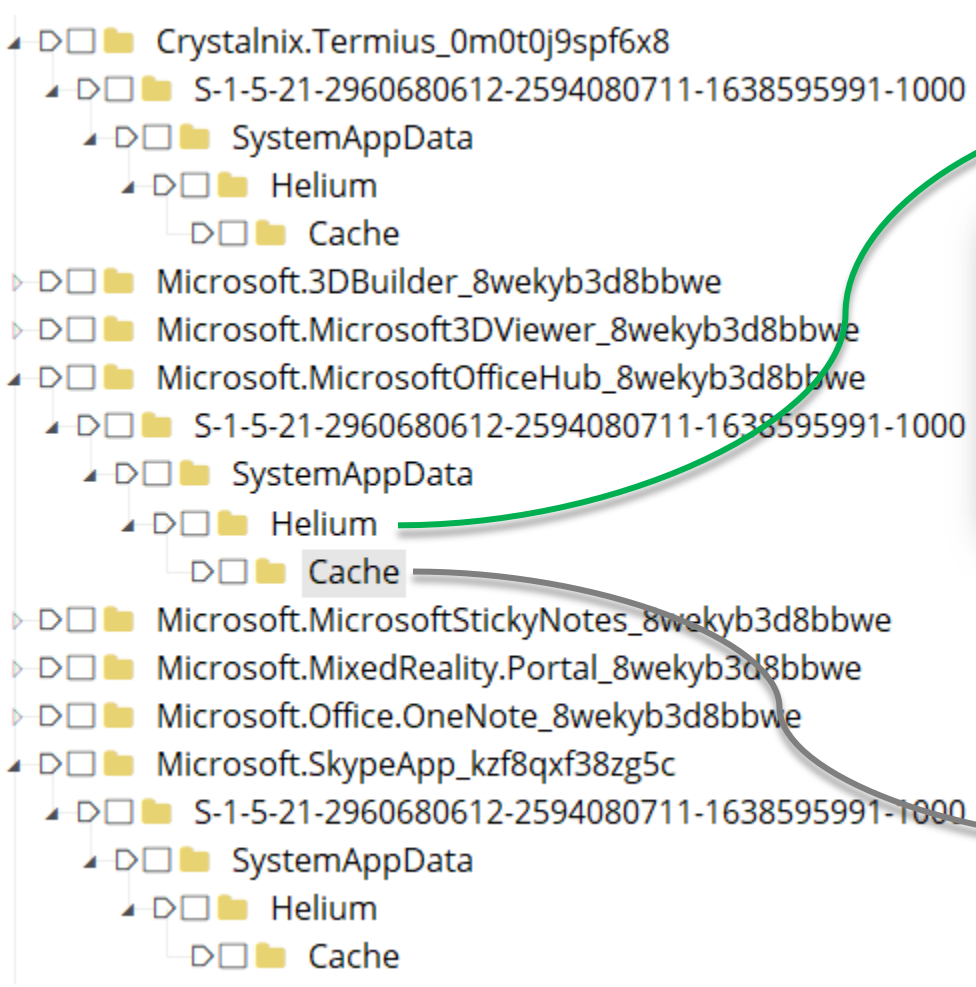
Source: https://docs.microsoft.com/en-us/windows/uwp/launch-resume/app-lifecycle

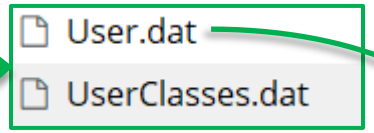
UsrClass.dat

- PersistedStorageItemTable reg key in
  - HKEY_CURRENT_USER\Software\Classes = Usrclass.dat
  - \Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\<App Pkg FamilyName>\PersistedStorageItemTable\ManagedByApp



More registry hives @ C:\ProgramData\Packages\<APP Family Name>

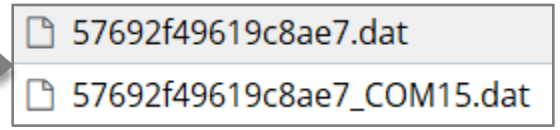




User info & artifacts here

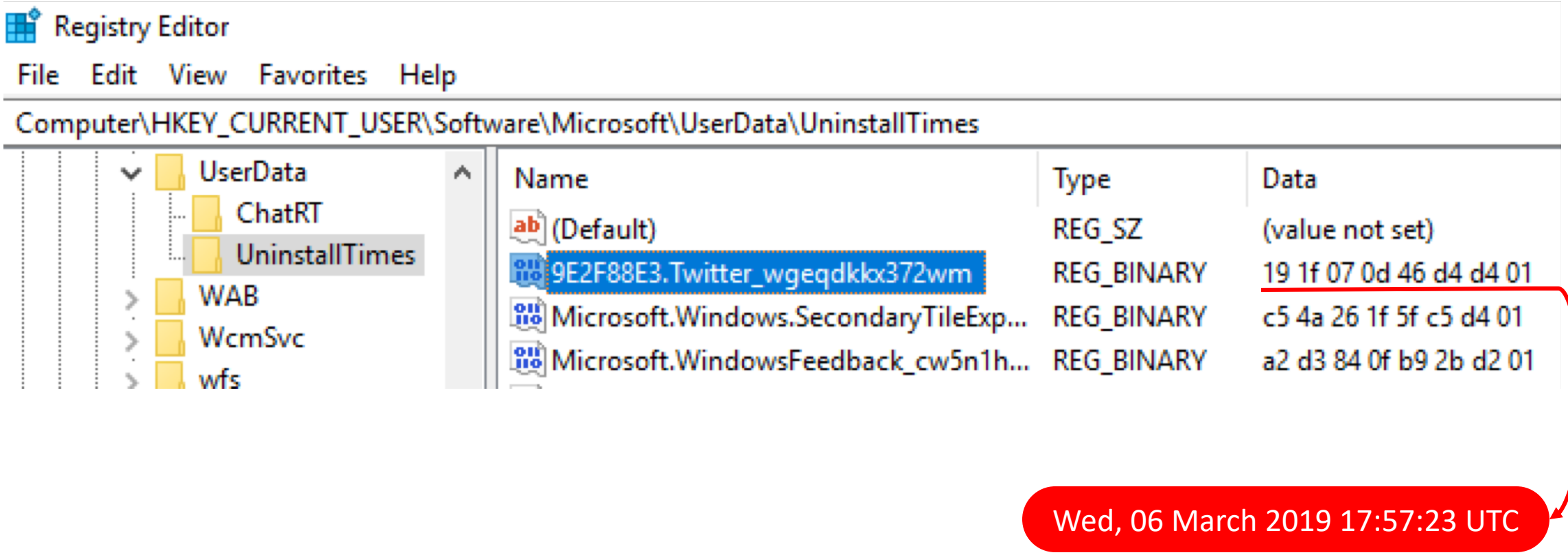
Program Name	Run Counter	Focus Count	Focus Time	Last Executed
Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim	1	2	0d, 0h, 02m, 04s	2019-03-07 14:23:15
UEME_CTLSESSION	237	912	0d, 11h, 30m, 40s	
Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	7	43	0d, 0h, 09m, 56s	2019-03-07 14:28:18

User.dat → Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

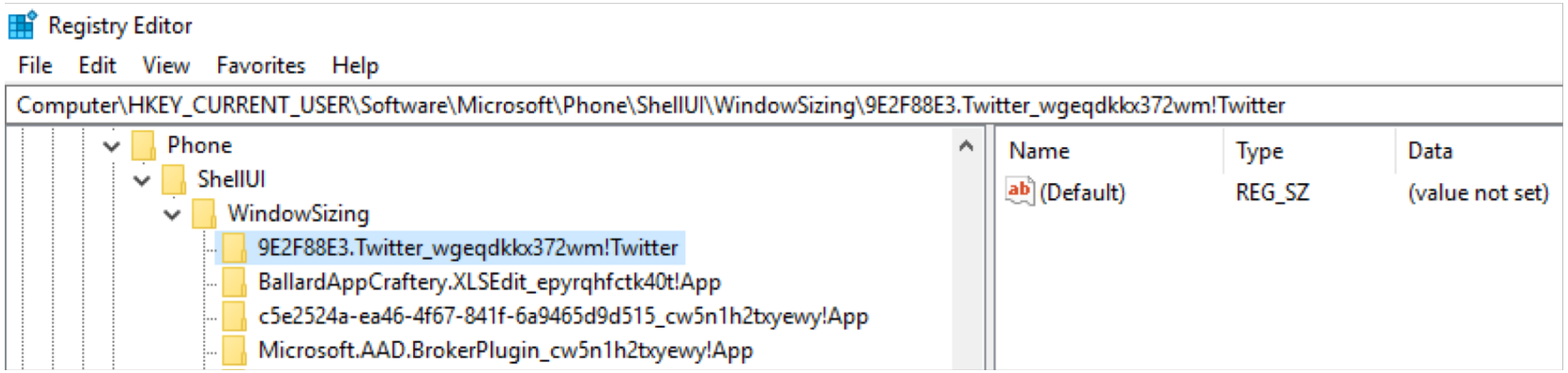


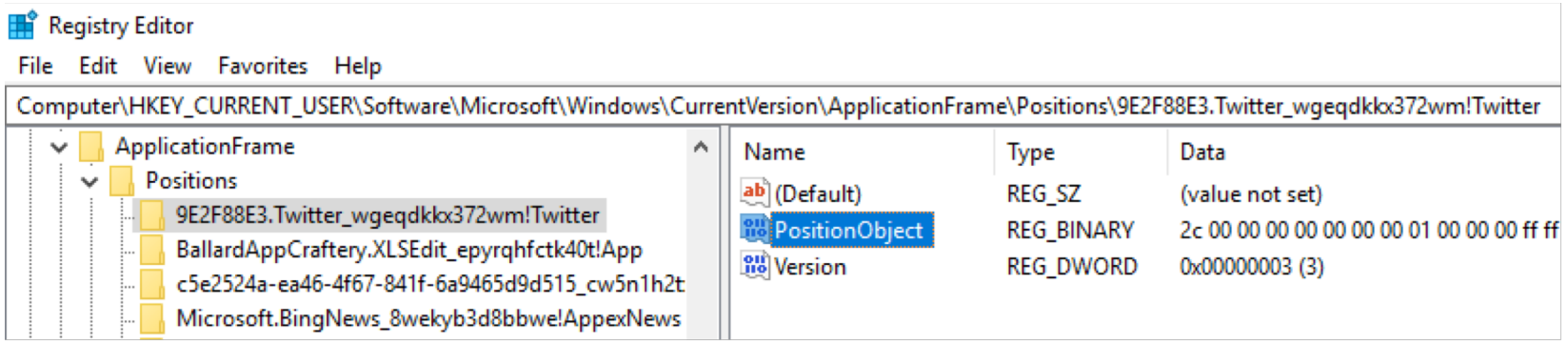
Mostly empty, no user artifacts

Remnants after uninstall



Leftovers..



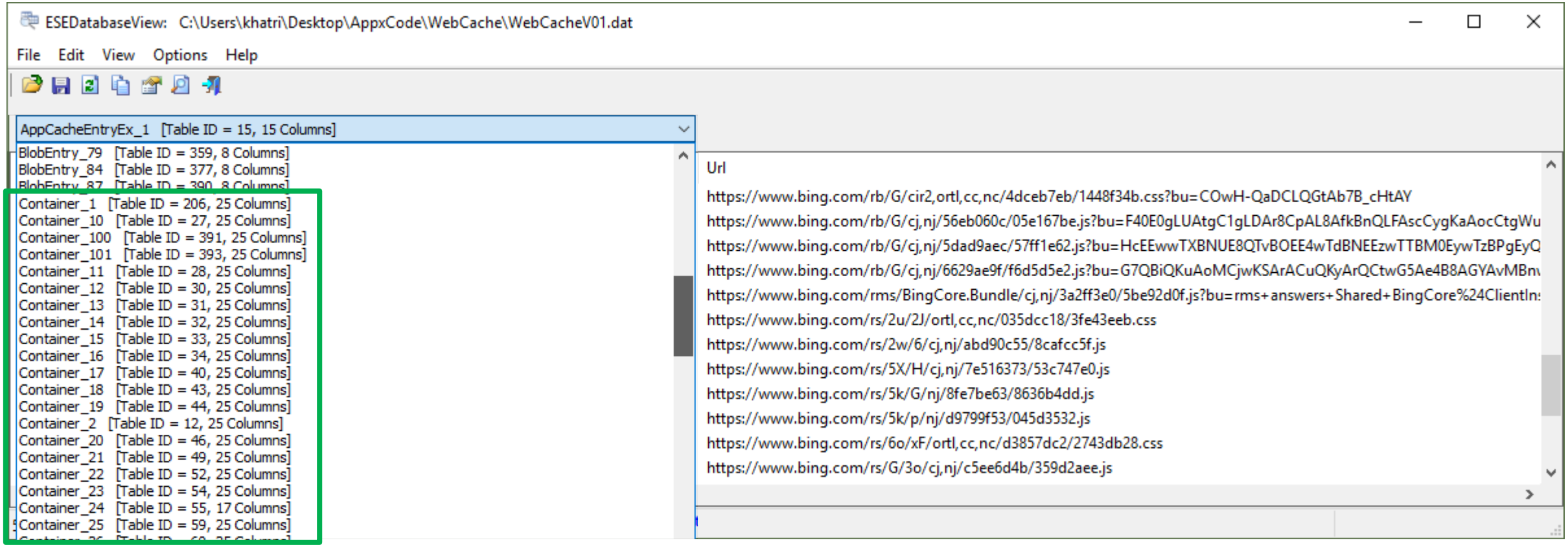


We found at least another 10 locations in the registry where you can find remnants of old Uninstalled Apps

These locations have to do with MrtCache, Push Notification settings, more window positioning and cached Capability settings

Webcache – IE/Edge database

- WebcacheV01.dat
  - C:\Users\<USER>\AppData\Local\Microsoft\Windows\WebCache\



PartitionsEx Table

TableId	Partition Type	PartitionId	Directory
9	0	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\AppCache\RBY7JROD
10	1	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCache\IE
19	4	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCache\IE
20	3	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCookies\ESE\
34	2	M	C:\Users\ROXY\AppData\Local\Microsoft\Windows\INetCache\IE
18	3	S-1-15-2-1063257880-1914585122-1954150059-946145533-116938067-416079064-1690466945	C:\Users\ROXY\AppData\Local\Packages\9e2f88e3.twitter_wgeqdkkx372wm\AC\INetCookies\ESE\
32	4	S-1-15-2-1609473798-1231923017-684268153-4268514328-882773646-2760585773-1760938157	C:\Users\ROXY\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\INetCache
33	3	S-1-15-2-1609473798-1231923017-684268153-4268514328-882773646-2760585773-1760938157	C:\Users\ROXY\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\INetCookies\ESE\

L=Low integrity, M=Medium

Table Names & Mapping

PartitionType value	Table holding data	Table content type
0	AppCacheEntryEx_*	Cached URL & file info
0	AppCacheEx_*	Cached URL & file info
1	DependencyEntryEx_*	Domains referenced by content in given URL
2	HstsEntryEx_*	Domain info?
3	CookieEntryEx_*	Cookie data
4	BlobEntry_*	Certificate blobs

18	3	S-1-15-2-1063257880-1914585122-1954150059-946145533-116938067-416079064-1690466945	C:\Users\ROXY\AppData\Local\Packages\9e2f88e3.twitter_wgeq72wm\AC\INetCookies\ESE\

CookieEntryEx_18 ← Resulting table name

Containers Table

- Provides data types & mapping for *Container_** tables

ContainerId	Name	PartitionId
1	Content	M
2	History	M
3	Cookies	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
4	Content	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
5	DOMStore	S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659745135-2630312742
6	Content	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
7	MicrosoftEdge_iecompat	M
8	MicrosoftEdge_iecompatua	M
9	Content	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723
10	Cookies	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723
11	BackgroundTransferApi	S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-1255436723

Querying **All_Container** view

```
SELECT App, Type, datetime((AccessedTime/10000000) -11644473600, 'unixepoch') AccessedTime, AccessCount, URL
FROM ALL_Container
```

App	Type	AccessedTime	AccessCount	Url
bingnews	DOMStore	2019-02-19 21:43:13	1	DOMStore:https://connexity.net/
bingnews	DOMStore	2019-02-19 22:12:03	1	DOMStore:https://www.incredibleindia.org/
bingnews	DOMStore	2019-02-19 21:22:45	1	DOMStore:https://ads.pubmatic.com/
xlsedit	Content	2019-03-14 20:56:06	3	http://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js
xlsedit	Content	2019-03-14 20:56:06	3	http://d1t2zu1r5z6kzt.cloudfront.net/cookies.js
xlsedit	Content	2019-03-14 20:52:29	1	http://cdn.softserver.co/v2/?flow=120&lang=en-US&uwp=true&slot=sheetedit
xlsedit	Content	2019-03-14 20:56:03	2	http://cdn.softserver.co/v2/?flow=121&lang=en-US&uwp=true&slot=sheetedit
xlsedit	Content	2019-03-14 20:56:06	1	http://static.fassets.net/creative/recycle-bin.png
xlsedit	Content	2019-03-14 20:55:31	2	http://static.fassets.net/creative/pdf/download-reader.gif
xlsedit	Content	2019-03-14 20:53:31	2	http://static.fassets.net/creative/download-notification.gif
xlsedit	Content	2019-03-14 20:52:31	2	http://static.fassets.net/creative/usb-icon.png
xlsedit	Content	2019-03-14 20:56:30	1	http://static.fassets.net/creative/winopener.gif
xlsedit	DOMStore	2019-03-14 20:52:29	1	DOMStore:http://cdn.softserver.co/
MicrosoftOfficeHub	History	2019-03-07 14:18:56	3	Visited: ROXY@https://contentstorage.osi.office.net/getofficecarouselcore/index
MicrosoftOfficeHub	History	2019-03-07 14:18:22	2	Visited: ROXY@https://odc.officeapps.live.com/odc/v2.0/hrd?lcid=1033&syslci

New Shiny Tools…

DEMO

Thanks for listening!

Any Questions?

Tools @ https://github.com/ydkhatri/Appx-Analysis

@swiftforensics
@jackfarley248

Yogesh@swiftforensics.com
Jack.Farley@mymail.champlain.edu

References to tools and resources

- Windows Internals Seventh Edition Part 1 - Pavel Yosifovich; David A. Solomon; Mark E. Russinovich; Alex Ionescu
- TokenView - https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools
- The Inner Workings of the Windows Runtime.pdf – James Forshaw
- Store and retrieve settings and other app data - https://docs.microsoft.com/en-us/windows/uwp/design/app-settings/store-and-retrieve-app-data
- ApplicationDataCompositeValueClass - https://docs.microsoft.com/en-us/uwp/api/windows.storage.applicationdatacompositevalue
- python-registry - https://github.com/willibal lenthin/python-registry
- Pares APPX programs - https://medium.com/@markmckinnon_80619/parse-the-appx-programs-in-autopsy-763d9017c4c
- All installed apps - https://boncaldoforensics.wordpress.com/2018/10/07/all-installed-apps-artifact-windows-10-forensics/
- App Lifecycle - https://docs.microsoft.com/en-us/windows/uwp/launch-resume/app-lifecycle